REMARKS

Claims 1-26 are pending in the present application. Claims 1, 3-6, 10-14, 19-21, 23, 24 and 26 have been amended herewith. Reconsideration of the pending claims is respectfully requested.

Amendments were made to the specification to correct errors and to clarify the specification. No new matter has been added by any of the amendments to the specification.

I. Objection to Drawings

The Examiner objected to the drawings, stating reference numbers 803-809 shown in Figure 8 are not described in the Specification. Applicants are amending the Specification herewith to include such reference numbers. Therefore, the objection to the drawings has been overcome.

II. Objection to Specification

The Examiner objected to the Specification, stating the Abstract contained too many words. Applicants are amending the Abstract herewith to reduce the word count. Therefore, the objection to the Specification has been overcome.

III. 35 U.S.C. § 102, Anticipation

The Examiner rejected Claims 1-26 under 35 U.S.C. § 102 as being anticipated by Sehr (US Patent 6,386,451 B1). This rejection is respectfully traversed.

With respect to Claim 1, Applicants urge that the cited reference does not teach (or otherwise suggest) that an electronic certificate added to the electronic document is itself encrypted. By encrypting this electronic certificate, it is possible to verify the authenticity of the electronic document during a subsequent decryption operation (Specification page 16, lines 21-26). It is also possible to verify or authenticate the user using this encrypted electronic certificate, as successful decryption of the electronic certificate means the proper user keys were used – thus verifying the user (Specification page 18, lines 1-7). This authenticity verification of both the document and user, which

is enabled by the encryption of the electronic certificate, is in addition to protecting the electronic document data through encryption, and also is in addition to the user electronic signature processing. Thus, this user authentication that is enabled by such electronic certificate encryption, which is in addition to the electronic signature mechanism, advantageously provides a two-level user authentication approach (Specification page 18, lines 1-7). The cited reference merely teaches that the document data itself is encrypted (col. 43, lines 58-59), and that a public key certificate can be attached to such data (col. 43, lines 62-64), to certify the passport as being issued by the agency. Such scheme does not provide any type of authenticity of the electronic document or user, which is advantageously provided by the claimed encryption (and subsequent decryption) of the certificate itself. Thus, it is urged that amended Claim 1 is not anticipated by the cited reference.

Applicants initially traverse the rejection of Claims 2-7 for reasons given above with respect to Claim 1 (of which Claims 2-7 depend upon).

Further with respect to Claim 3, Applicants urge that the cited reference does not teach the claimed feature of "wherein the electronic document contains a unique serial number from an issuing authority that uniquely identifies the electronic document". In rejecting Claim 3, the Examiner states that the unique serial number is taught by the cited reference at col. 43, lines 53-57. Applicants urge that this passage describes security information that is unique to a rightful passport-holder – i.e. *unique to the user of the card* – such as a social security number or signature, which is used as a further means of protecting data in the card. In contrast, Claim 3 is directed to a unique serial number which advantageously provides an ability to track the electronic document. Applicants have amended Claim 3 to further clarify this distinction.

Further with respect to Claim 4, Applicants urge that the cited reference does not teach the claimed feature of "wherein the electronic document contains a digital watermark". In rejecting Claim 4, the Examiner states that the digital watermark is taught by the cited reference at col. 43, lines 55-65. Applicants urge that this passage describes (1) requiring a passenger to provide a matching social security number or signature before a new passport can be downloaded, and (2) encrypting of passport data with a secret key or passenger biometrics, where the passenger must provide the secret

key or matching biometrics in order to download and unlock the passport data. In both cases, these passages describe an action that must occur before the passport data can be downloaded – i.e. an access control mechanism. In contrast, Claim 4 is directed to characteristics of the electronic document itself, and specifically recites that the electronic document contains a digital watermark. The cited reference does not teach or otherwise suggest any document that contains a digital watermark. Thus, it is urged that Claim 4 has been erroneously rejected by the Examiner.

Further with respect to Claim 5, such claim has been amended in accordance with the Specification on page 15, lines 12 – 22, and now recites "wherein the electronic document comprises an authorization seal from the issuing authority that is displayed by the pervasive computing device to verify authenticity of the electronic document". The cited reference does not teach or otherwise suggest this claimed feature, but instead merely describes that the cardholder has the option to choose from various text, logos, artworks, or audio and video files provided by the center, where the compiled information and selected options can be loaded into or imprinted onto the passenger card (col. 10, lines 19-24). Such information is not used as a part of authenticity verification of the electronic document, as expressly recited in Claim 5. Thus, it is urged that amended Claim 5 is not anticipated by the cited reference.

Further with respect to Claim 7, Applicants urge that the cited reference does not teach the claimed feature of "wherein the electronic document is renewed automatically at set time intervals". In rejecting Claim 7, the Examiner asserts that this feature is taught by the cited reference at col. 43, lines 60-67. Applicants show error, as such passage merely describes overwriting old passport data with new data responsive to a user's manual passport renewal, and automatically canceling old passport data if a predetermined condition such as an expiration date is met. Thus, this passage teaches a manual overwrite of new data, and an automatic cancellation of old data. In contrast, Claim 7 is directed to an automatic renewal of the electronic document. An *automatic cancellation* of old data, as taught by the cited reference, does not teach or otherwise suggest an *automatic renewal* of the electronic document, as claimed. Thus, it is shown that Claim 7 has been erroneously rejected as every element of the claimed invention is not identically shown in a single reference.

With respect to Claim 8, such claim recites a method for verifying the authenticity of an electronic identification document, and includes steps of (i) validating a digital certificate attached to the electronic document, and (ii) verifying the authenticity of an electronic signature attached to the electronic document. As can be seen, Claim 8 advantageously provides two aspects of verifying the authenticity of the electronic document. First, a digital certificate that is attached to the electronic document is validated. In addition, the authenticity of an electronic signature that is attached to the electronic document is verified. In rejecting the digital certificate validation aspect of Claim 8, the Examiner cites Sehr col. 1, lines 48-51, and col. 42, lines 14-21; and in rejecting the electronic signature aspect of Claim 8, the Examiner cites col. 18, lines 30-35. Applicants show two-fold error in such assertion. First, the passage cited at col. 1 does not teach any operation steps at all, and thus does not teach either of these two recited steps; the passage cited at col. 42 merely describes comparing selected card data against information maintained by the government, and does not teach any type of *digital certificate validation* or verification of the *authenticity of an electronic signature.* Secondly, these three cited passages describe different aspects of the Sehr system, and these passages do not synergistically co-act with one another as part of an overall process of verifying the authenticity of an electronic identification document. Thus, it is urged that the cited reference does not teach (or otherwise suggest) *both* (i) validating a *digital certificate* attached to the electronic document, *and* (ii) verifying the authenticity of an *electronic signature* attached to the electronic document as a part of an overall process of verifying the authenticity of an electronic identification document. Rather, the Sehr card is authenticated by use of an authenticity code stored in the card which can be compared against a file stored in a database (col. 18, lines 15-23). Thus, it is urged that Claim 8 has been erroneously rejected, as every element of Claim 8 is not identically shown in a single reference.

Still further with respect to Claim 8, which is directed to a method for verifying the authenticity of an electronic document, such claim includes steps of decrypting of the electronic document and decrypting of the electronic document as a part of the authenticity verification. In rejecting this aspect of Claim 8, the Examiner cites two unrelated passages as teaching the claimed encryption and decryption steps. As to the

decrypting step, the Examiner cites col. 42, lines 14-21. Applicants urge that this passage does not describe any decrypting operation whatsoever, but rather merely describes that a module 'automatically verifies' card-based data without describing how such verification is done. This passage also states that selected card data can be 'compared' against information maintained by government agencies, but this compare of information does not teach or otherwise suggest any step of decrypting, as expressly recited in Claim 8. As to the claimed encrypting step – which is a part of the document authenticity method – the Examiner cites col. 1, lines 48-51 as teaching this claimed step. Applicants show two-fold error in such assertion. First, the cited passage at col. 1 merely states that certain programs include cryptographic schemes, digital signatures and authenticity codes to protect against fraudulent use. This passage does not teach or otherwise suggest using *an encryption step as a part of verifying document authenticity*. Second, these two cited passages are disjoint passages that do not synergistically co-act together. Claim 8 recites both a decryption step and an encryption step being used synergistically together as a part of the overall document authenticity verification. The cited reference does not teach or otherwise suggest using both decryption and encryption steps to verify document authenticity. Instead, the cited reference teaches that the document's authenticity is verified by an authenticity code that is stored on the card, and when the card is presented for service, the card can be validated via this code by comparing the code against an authenticity file stored in the issued database or by performing a self-test of the card-based code (col. 18, lines 14-23). This is a substantially different authenticity verification technique from what is recited in Claim 8. The cited reference also describes a passport verification technique at col. 34, lines 25-35. There, it states that the passport is retrieved from the passenger card and viewed on a display screen, with optional check of the user's signature. Again, this is substantially different than the authenticity verification technique recited in Claim 8. Thus it is shown that Claim 8 has been erroneously rejected, as every element of the claimed invention is not identically shown in a single reference.

Applicants initially traverse the rejection of Claims 9-18 for reasons given above with respect to Claim 8 (of which Claims 9-18 depend upon).

Applicants further traverse the rejection of Claim 10 for similar reasons to the further reasons given above with respect to Claim 3.

Applicants further traverse the rejection of Claim 11 for similar reasons to the further reasons given above with respect to Claim 4.

Applicants further traverse the rejection of Claim 12 for similar reasons to the further reasons given above with respect to Claim 5.

Further with respect to Claim 13, Applicants urge that the cited reference does not teach the claimed step of "changing information contained in the electronic document after decrypting the electronic document, wherein the changes are a part of the electronic document when the electronic document gets encrypted by the encrypting step". Claim 13 has been amended to further clarify that the changing of information is with respect to the electronic document after being decrypted and prior to being encrypted.

Further with respect to Claim 14, Applicants urge that the cited reference does not teach the claimed step of "attaching new information to the electronic document after decrypting the electronic document, wherein the new information is a part of the electronic document when the electronic document gets encrypted by the encrypting step". Claim 14 has been amended to further clarify that the attaching of new information is with respect to the electronic document after being decrypted and prior to being encrypted.

With respect to Claim 19 (and dependent Claim 20), Applicants traverse for similar reasons to those given above with respect to Claim 1.

With respect to Claim 21, Applicants traverse for similar reasons to those given above with respect to Claim 1.

With respect to Claim 22, Applicants traverse for similar reasons to those given above with respect to Claim 8.

With respect to Claim 23, Applicants traverse for similar reasons to those given above with respect to Claim 19.

With respect to Claim 24, Applicants traverse for similar reasons to those given above with respect to Claims 3 and 4.

With respect to Claim 25, Applicants traverse for similar reasons to those given above with respect to Claim 8.

With respect to Claim 26, Applicants traverse for similar reasons to those given above with respect to Claims 3, 4 and 19.

Therefore, the rejection of Claims 1-26 under 35 U.S.C. § 102 has been overcome.

IV. Conclusion

It is respectfully urged that the subject application is patentable over the cited reference and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: 4/13/05

Respectfully submitted,

Duke W. Yee
Reg. No. 34,285
Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorneys for Applicants